Michigan Department of Human Services

# CSA

Children's Services Administration Communication Issuance

**Type:** ☐ Informational Memorandum (IM)
☒ Program Instruction (PI)
☐ Policy Guide (PG)

**Issuance Date:** 08/19/13 **Obsolete Date:** n/a

**Response Due:** 08/30/13

**Log No.:** 13-102

**Contact:** Lisa Kinkema; misacwis@michigan.gov

**Originating Office:** MiSACWIS Project Office

**Subject/Title:** MiSACWIS Security Web-Based Training (WBT)

**Distribution:**
☒ DHS Child Welfare Staff
☒ Private Agency Child Welfare Staff
☒ CSA Central Office Managers/Staff
☐ Native American Tribes
☐ Data Management
☒ DHS County Directors
☐ Adult Services Staff
☒ Other: Contracted Residential Agencies

☒ BCAL
☒ CWTI
☒ SACWIS

The Office of Workforce Development and Training (OWDT), in conjunction with the Michigan Statewide Automated Child Welfare Information System (MiSACWIS) staff, have developed a web-based training (WBT) on security requirements in MiSACWIS. The ***MiSACWIS Security Training*** WBT is posted to Omni-Track Plus (OTP) under the MiSACWIS > Introduction to MiSACWIS folder. There are no pre-requisites for this WBT. The link to the Child Welfare Training Institute webpage is:
http://www.michiganchildwelfaretraining.com/

Per the contract amendment with private foster care, adoption and residential agencies, all staff must complete this training prior to the statewide implementation of MiSACWIS in October 2013. DHS staff must also complete this training as it applies specifically to MiSACWIS security awareness. A benefit to taking the WBT is anyone who completes the training with a passing score of 90 percent will receive 1 hour of in-service training credit.

**MiSACWIS and Confidential Information**

MiSACWIS is a statewide system with a large amount of confidential data. The system includes children's protective services (CPS), adoption, Internal Revenue Service (IRS), Social Security and protected health information. DHS must ensure that federal and state security, confidentiality, and privacy laws are followed.

The main focus of the security training is on the IRS requirements, as MiSACWIS will contain IRS data. Once IRS data is in the system, the IRS considers the data to be "co-mingled" and all of the system data then falls under the IRS regulations for security. Furthermore, all of the security precautions mentioned in the IRS videos apply to all confidential data in MiSACWIS. Many of the IRS security requirements fall on the state and its infrastructure; therefore, the security training is focused on the end-user and their access to confidential information.

All MiSACWIS users, even those DHS staff who have had access to the statewide system for years, will have access to additional confidential data available in MiSACWIS. Information is the key to providing good services for our clients. Therefore, it is very important that all users understand that they have a responsibility to protect this information. Users may lose the privilege of accessing MiSACWIS if they inappropriately release

confidential information. Civil and criminal penalties may also apply depending on the applicable laws and regulations.

Moreover, it is important for all users who are working outside of their office to follow good security practices. Security requirements are more easily met when users store data in the secure MiSACWIS application instead of storing locally or printing the information. Additionally, it is essential that users keep passwords protected and are aware of any potential for unauthorized persons viewing MiSACWIS screens when accessing the system. Another very important security provision includes only using the MiSACWIS application for work purposes – users must not look up their neighbors, relatives, friends, etc., on the system. Furthermore, all users must notify management of any potential conflicts of interest or security breaches.

**Authorized Requesters and Local Office Security Coordinators**

To ensure that only authorized users obtain access to MiSACWIS, each private agency and residential agency must have an authorized requester. Central office security will not grant anyone access to MiSACWIS unless the authorized requester has signed the Non-DHS 60 form. Private agencies already have identified a person to fulfill this role.

With the implementation of MiSACWIS, contracted residential agency payment roster approvers will also access the system. Therefore, all contracted residential agencies must also identify at least one authorized requester per agency. Residential agencies must submit the name(s) and contact information for their authorized requester to Amanda Doane via email at DoaneA@Michigan.gov by **August 30, 2013.**

The Local Office Security Coordinators (LOSCs) fulfill this function for DHS offices. They will enter DHS staff in the MiSACWIS application. MiSACWIS project staff is developing an LOSC Guide with step-by-step procedures for adding or inactivating staff profiles and user groups in MiSACWIS. (Reference ***Attachment A*** for additional duties of the authorized requester and the LOSC.)

**MiSACWIS Security and Confidentiality Requirements**

Central office application security staff is revising the security agreement for MiSACWIS users. There will be two separate forms:

1. The *Staff Profile Security Agreement* (DHS 60) DHS County and Central Office Employees.
2. The *Staff Profile Security Agreement* (DHS 60 Non-DHS) for Non-DHS staff.

By signing the form and accessing the MiSACWIS application, all MiSACWIS users agree to comply with the following requirements:

- All Federal and State laws regarding the use of computers and dissemination of information obtained from their use, including but not limited to the SOM Computer Crime Law (1979 PA 53, MCL 752.79 through MCL 752.797, MSA 28.529(1) through (7) to perform my job function to the exclusion of all other uses. These requirements can be found at: http://www.legislature.mi.gov/(S(yppr1h45i5qjx255pcb4lnaq))/mileg.aspx?page=MclPASearch.
- The Michigan State Government Network Policy Procedures 1410.17 at: http://www.state.mi.us/adminguide/1400/1410-17.htm.
- The 1460.00 Acceptable Use of State of Michigan Department of Technology, Management and Budget at: http://www.michigan.gov/documents/dmb/1460.00_184733_7.pdf
- Security Breach Procedures, 1340.00.00.02 (Reference ***Attachment B***).

- Storage of Sensitive Information on Mobile Devices Standard, 1340.00.06. (Reference ***Attachment C*** – this document references SOM Administrative Guide Procedure 1350.90 for data sanitation and media disposal. This document may be found at: http://www.michigan.gov/documents/dmb/1350.90_184606_7.pdf).
- MiSACWIS Privacy Policy (Reference ***Attachment D***).
- The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); HIPAA's implementing regulations, as amended, 45 CFR Parts 160-164; and any other applicable federal or state privacy and/or confidentiality laws.

Additional security and confidentiality laws and regulations are included within the security training WBT.

Earlier this year, the MiSACWIS project staff worked with the MiSACWIS liaisons to clean up all of the current SWSS users and ensure they were correctly profiled in SWSS. MiSACWIS project staff will send out one final SWSS staff profile report around the end of August to ensure that the profiles are correct prior to conversion to MiSACWIS. Private agency staff are also submitting DHS-60s to Central Office Security to add staff who do not have a current work need to access SWSS, but will be put in a SWSS conversion queue to be ready for MiSACWIS conversion.

Anyone with an existing staff profile in SWSS will be converted to MiSACWIS. It will not be necessary to complete a new security form for existing SWSS users. MiSACWIS project staff will send out spreadsheets to the MiSACWIS liaisons closer to the time of statewide implementation so the applicable MiSACWIS security users groups can be selected for all SWSS users. For example, in SWSS, a worker has a Foster Care staff profile; in MiSACWIS, this user will have the Child Foster Care Specialist user group. MiSACWIS liaisons will need to work with their office/agency management to select the appropriate user groups for all staff. The spreadsheet will include definitions for all of the MiSACWIS user groups.

Any new MiSACWIS users, including the residential agency staff who will be the payment roster verifier, will need to complete a new form **after** the implementation of MiSACWIS. These new forms and information about all MiSACWIS users accessing applicable InfoView reports in the data warehouse will be released closer to the MiSACWIS implementation via a new communication issuance (CI).

Any questions on the MiSACWIS security training can be submitted to the identified MiSACWIS liaison. The liaison may then send inquiries to the MiSACWIS@michigan.gov email address. Security-related questions may be submitted to Central Office Security at DHS_Application_Security@michigan.gov.

**Attachment A: Duties of the Authorized Requester and the Local Office Security Coordinator (LOSC)**

The duties of the contracted-private agency and -CCI authorized requesters include:

1. Review, approve, and certify all Staff Profile Security Agreements (DHS-60 Non-DHS) for staff.
2. Maintain a copy of all *Staff Profile Security Agreement* (DHS-60 Non-DHS) requests.
3. Report all changes to the DHS children services liaison (e.g., a new authorized requestor, locations, license number, etc.) by contacting the BCW contract analyst.
4. Within 24 hours of a MiSACWIS user's departure from employment, notify DHS Application Security via email: DHS_Application_Security@michigan.gov. Staff departures include any extended leave of absence.
5. Immediately notify DHS Application Security via email at DHS_Application_Security@michigan.gov of the following:
    a. All suspected unauthorized use of the MiSACWIS application, and/or
    b. Users who are terminated for cause.
6. Establish policy consistent with the State of Michigan DHS security policies that are distributed to all employees, along with the provision of security awareness training and documentation of the training attendance. The policies must include but are not limited to the following:
    a. Prohibit the sharing of authentication information, e.g., passwords and PINs.
    b. Limit users' access to authorized uses.
    c. Prohibit unauthorized people from viewing MiSACWIS case information.
    d. Users' agreement to protect the sensitive and confidential information in MiSACWIS.
    e. Requirement that erroneously created confidential information must be shredded or otherwise destroyed.
    f. Confidential documents, forms, and negotiable documents must be stored, controlled, and periodically inventoried.
    g. MiSACWIS documents are handled and retained in accordance with laws, orders, directives, and DHS policies.
    h. MiSACWIS must only be accessed by users on a "work-issued" device, e.g., laptop, desktop, etc.
    i. Per DHS' instruction, allow access to MiSACWIS by state- and federal-agency staff for the purposes of an audit or other necessary evaluations.
    j. The Contractor agrees to comply with all terms and conditions that DHS establishes regarding the Contractor's use and access to the MiSACWIS application system. The Contractor shall comply with all Federal and State laws regarding the use of computers and dissemination of information obtained from their use, including but not limited to the SOM Computer Crime Law (1979 PA 53, MCL 752.79 through MCL 752.797, MSA 28.529(1) through (7) to perform all responsibilities contained in this Agreement to the exclusion of all other uses. In addition all users of the State of Michigan DHS automated systems must read and agree to comply with:
        i. The Michigan State Government Network Policy Procedures 1410.17 at: http://www.state.mi.us/adminguide/1400/1410-17.htm
        ii. The 1460.00 Acceptable Use of State of Michigan Department of Technology, Management and Budget at: http://www.michigan.gov/documents/dmb/1460.00_184733_7.pdf
        iii. Security Breach Procedures, 1340.00.00.02
        iv. Storage of Sensitive Information on Mobile Devices Standard, 1340.00.06.
        v. MiSACWIS Privacy Policy.

vi. The Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (HIPAA); HIPAA's implementing regulations, as amended, 45 CFR Parts 160-164; and any other applicable federal or state privacy and/or confidentiality laws. Contractor shall assure that HIPAA's Privacy and Security Rules are communicated and enforced, and that users are properly trained and informed of their responsibilities.

The DHS LOSC's duties include:

1. Review, approve, and certify all Staff Profile Security Agreements (DHS-60) for staff.
2. Maintain a copy of all *Staff Profile Security Agreement* (DHS-60) requests.
3. Within 24 hours of a MiSACWIS user's departure from employment, inactivate the user's security to the MiSACWIS application. Staff departures include any extended leave of absence.
4. Immediately notify DHS Application Security via email at DHS_Application_Security@michigan.gov of all suspected unauthorized use of the MiSACWIS application.

| DTMB Technology, Management & Budget | *State of Michigan*<br>*Department of Technology, Management & Budget* | |
|---|---|---|
| **Subject:** | **How To Handle A Breach of Personal Identifiable/Sensitive Information Incidents** | **Procedure Number** |
| **Authoritative Policy:** | 1340.00 Information Technology Information Security | **1340.00.01.02** |
| **Standard Number:** | TBD | |
| **Distribution:** | Statewide | |

**Purpose:**

To establish a formal statewide Notification of Breach procedure in the event of a security breach where a state agency who owns or licenses computerized data that include Personal Identifying/Sensitive Information, to notify without reasonable delay each Michigan resident for whom personal identifying information (encrypted or unencrypted) was accessed and acquired or reasonably believes that the information was accessed or acquired by an unauthorized person.

The public rightly assumes and should be assured that the data in the possession of Michigan State Government is secure and protected from unauthorized disclosure or misuse.

This procedure outlines the process for reporting and responding to a security incident where there is a potential breach of personal identifying information that is collected by, on behalf of or in the custody of the State of Michigan (SOM).

Information covered by this procedure may be in written or printed form or may reside electronically on traditional devices such as mainframes, servers and personal computers (desktop and laptop), on newer devices such as USB keys, PDAs, BlackBerrys and cell phones, or other state-of-the-art devices that may be developed. These devices may be state owned or may be owned by an employee or vendor.

**Owner:**

DTMB Office of Enterprise Security (OES)

**Procedure:**

| Who | Does What |
|---|---|
| Discovering Agency Employee | 1. Is notified or discovers a potential breach of SOM Personal Identifying Information.<br>2. Immediately reports any instance of potential breach of SOM Personal Identifying Information to immediate supervisor/manager. |

| DTMB Technology, Management & Budget | *State of Michigan*<br>*Department of Technology, Management & Budget* | |
|---|---|---|
| **Subject:** | **How To Handle A Breach of Personal Identifiable/Sensitive Information Incidents** | **Procedure Number** |
| **Authoritative Policy:** | 1340.00 Information Technology Information Security | **1340.00.01.02** |
| **Standard Number:** | TBD | |
| **Distribution:** | Statewide | |

| | |
|---|---|
| Discovering Agency Management | 3. Follows discovering Agency's internal policy and procedure for incident reporting.<br><br>4. Reports the potential breach through the proper chain of command to the appropriate internal Agency Deputy Director and their Department of Technology, Management, & Budget (DTMB) Agency Information Officer (IO) within 24 hours of discovering the potential breach. |
| Agency Deputy Director | 5. Performs initial assessment and determines if the potential breach requires further investigation.<br><br>6. If it is determined that further investigation is required, and If the incident occurred before 5:00pm, contacts their DTMB Agency IO and the DTMB Chief Information Security Officer (CISO)/DTMB Office of Enterprise Security (OES) for assistance.<br>Go to step 8.<br><br>If the incident occurs after 5:00pm, calls the DTMB Client Service Center (CSC) and submits a remedy ticket within 24 hours of notification of the potential breach.<br><br>**Reports the following information to the CSC:**<br>Date and time of potential breach<br>Contact person name and number<br>Type of data that maybe involved in the potential breach<br>Device PII stored on (laptop, USB, PDA, etc.)<br><br>**Department of Technology Management & Budget**<br>Client Service Center(CSC)<br>(517) 241-9700 or (800) 968-2644 |
| DTMB Client Service Center(CSC) | 7. Completes the remedy ticket and assigns the remedy ticket to DTMB Office of Enterprise Security (OES). |

| DTMB Technology, Management & Budget | *State of Michigan Department of Technology, Management & Budget* | |
|---|---|---|
| **Subject:** | **How To Handle A Breach of Personal Identifiable/Sensitive Information Incidents** | **Procedure Number** |
| **Authoritative Policy:** | 1340.00 Information Technology Information Security | **1340.00.01.02** |
| **Standard Number:** | TBD | |
| **Distribution:** | Statewide | |

| | |
|---|---|
| CISO/Office of Enterprise Security | 8. Initiates an investigation to determine the nature and scope of the incident.<br><br>9. Provides preliminary finding to Agency Deputy Director within 24 hours of the CISO being informed or receiving the remedy ticket. |
| Agency Deputy Director | 10. If after reasonable investigation, the Agency's Deputy Director determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state. Documents the incident, determine the scope of the potential breach, and review internal control to ensure integrity, security and confidentiality of the data system.<br><br>11. If after reasonable investigation, the Agency's Deputy Director determines that the security breach has or is likely to cause substantial loss or injury to, or result in identity theft with respect to, 1 or more residents of this state, the Agency's Deputy Director informs the Agency Director of the scope of the breach. The Agency Director shall:<br><br>A.) Immediately contacts the Governor's Communications Office to plan the response to the media.<br>B.) Immediately contacts other Agencies potentially affected (i.e. Treasury/Credit Card Information, MSP/LEIN information, Dept. of State/Driver License information, etc.).<br>C.) Compose the appropriate notice of breach response to the affected person or party in compliance with step # 12 of this procedure) and subsection 12 of Identity Theft Protection Act (Public Act 566 of 2006), without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information, determine the scope of the breach, and restore the reasonable integrity, security, and confidentiality of the data system. |

| DTMB Technology, Management & Budget | *State of Michigan Department of Technology, Management & Budget* | |
|---|---|---|
| **Subject:** | **How To Handle A Breach of Personal Identifiable/Sensitive Information Incidents** | **Procedure Number** |
| **Authoritative Policy:** | 1340.00 Information Technology Information Security | **1340.00.01.02** |
| **Standard Number:** | TBD | |
| **Distribution:** | Statewide | |

| | |
|---|---|
| | 12. The notice shall be clear and conspicuous. The notice shall include a description of the following:<br><br>The incident in general terms;<br>A.) The type of personal identifying information that was subject to the unauthorized access and acquisition;<br>B.) The general acts of the state to protect the personal identifying information from further unauthorized access;<br>C.) A telephone number or web site that the person may call or access for further information and assistance, if one exists; and<br>D.) Advice that directs the person to remain vigilant by reviewing; account statements and monitoring personal credit reports. |

**Approving authority:**

Rich Reasner, Acting OES Director: (signed by Director Reasner) Date: (revision 3/30/11)

| DTMB Technology, Management & Budget | *State of Michigan*<br>*Department of Technology,*<br>*Management & Budget* | |
|---|---|---|
| **Subject:** | **Storage of Sensitive Information on Mobile Devices and Portable Media (former Ad Guide 1315.00)** | **Standard Number** |
| **Authoritative Policy:** | **1340 IT Information Security Policy** | **1340.00.06** |
| **Procedure Number:** | TBD | |
| **Distribution:** | Statewide | |

**Purpose:**

To establish a statewide standard for the protection of State of Michigan (SOM) sensitive information and data stored on mobile devices and portable media.

The public rightly assumes and should be assured that the data in the possession of Michigan state government is secure and protected from unauthorized disclosure or misuse.

Any user who has been authorized to access SOM sensitive information has an obligation to safeguard and protect the confidentiality of such data. The objective of this standard is to minimize the likelihood that sensitive or confidential SOM information is inadvertently disclosed.

**Contact/Owner:** DTMB CyberSecurity and Infrastructure Protection (CIP)

**Scope:** Executive Branch Departments and Sub-units, private partners and contractors.

**Standard:**

Storage of sensitive information on mobile devices or portable media is permitted only if all of the following requirements have been satisfied:

1. Use is restricted to individuals whose job duties require it.
2. Granted for a finite duration as needed to fulfill the specific functions required to perform a specific job.
3. Approval has been obtained by both the employee's department head (or their designee) and the system/data owner. For non-SOM employees, "department" is defined as the SOM Agency contracting with the 3rd party.
4. Sensitive data has been encrypted. Encryption must comply with the DTMB Standard 1340.00.07 as published. **Unencrypted storage of sensitive information on mobile devices and portable media is prohibited.** Please note that SOM Administrative Guide Procedure 1350.90 for data sanitation and media disposal will need to be followed.

ANY instance of SOM sensitive information (including that stored on a mobile device or portable media – encrypted or unencrypted) being lost, stolen, or where there is reasonable belief that an unauthorized person may have acquired the data, **must be reported immediately** to your appropriate Agency management and the Department of Technology, Management and Budget's Customer Service Center at (517) 241-9700 or (800) 968-2644.

Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment and/or criminal prosecution where the act constitutes a violation of law.

Any third party found to have violated this standard may be subject to action, up to and including criminal prosecution where the act constitutes a violation of law. A breach of contract and fiduciary liability may also apply.

**Definitions:**

### Data/System Owner
Senior management of the Agency that is ultimately responsible of ensuring the protection and appropriate use of their business' data.

### Encryption
The translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key that enables you to decrypt it.

### Mobile Devices
Any mobile device (State-owned or privately-owned) capable of storing data. Examples include, but are not limited to: laptops, tablet PCs, Blackberrys, cell phones, PDAs, IPods, and players.

For the purpose of this standard, all non-state-owned computing or data storage equipment (*e.g.*, PC, server, Network Attached Storage (NAS), and Storage Area Network (SAN)) are considered mobile devices.

### Portable Media
Any portable media (State-owned or privately-owned) capable of storing data. Examples include, but are not limited to: external hard drives, USB thumb drives, flash drives, memory sticks and cards, CDs, DVDs, and floppy disks.

### Sensitive Information and Data
Those data elements that are governed or restricted in some manner by a federal or state statue, rule, policy or requirement. At a minimum, sensitive information that all agencies must encrypt includes (but is not limited to):

1. Name and social security number pair.
2. Name and credit card number pair.
3. Personal health records as identified by HIPAA.

In addition to above, agencies may assign data classifications to their data elements. Encryption would be required for all Agency-specific information labeled sensitive.

**Approving authority:**

John Nixon, CPA (signed by Director Nixon) Date: (revision 4/28/12)

## MiSACWIS Privacy Policy

When you access MiSACWIS, we may gather information in the following ways:

- **Information collected automatically**. When you access MiSACWIS, some of your information is automatically collected. This may include information about how you linked to MiSACWIS, when you accessed our website, the searches you initiated, things you clicked on, your IP address, the type of browser and operating system you used, and the pages you requested and visited.

- As a MiSACWIS user, you must provide the State of Michigan with your name, employment address, employment phone number, and employment email address. The State of Michigan will assign you a unique username, and password.

### Cookies

Michigan.gov uses "cookies" to customize your browsing experience. A cookie is a small text file that is saved on your computer when you visit a website.

Session cookies allow you to move through many pages of a website quickly and easily without having to authenticate or reprocess each new area you visit. Session cookies are destroyed after successful completion of a transaction, after a few minutes of inactivity, or when the browser is closed.

Persistent cookies help websites remember your information and settings when you visit them in the future. They continue to exist after a few minutes of inactivity, after the browser is closed, or after a user completes a single session.

MiSACWIS uses cookies to maintain your logged in session.

### Sharing information

We will only share personal information about you with others if:

- We have your consent to share the information, or
- We are authorized to do so by law. e.g., to respond to subpoenas, court orders, legal process, or to requests pursuant to a statute requiring or permitting disclosure such as the Michigan Freedom of Information Act, MCL 15.231, *et seq.*

### Security

We limit access to personally identifiable information gathered through MiSACWIS to employees and agents who need access to perform a specific job. Security measures have been integrated into the design, implementation, and day-to-day operations of MiSACWIS as part of our continuing commitment to the security of electronic content as well as the electronic transmission of information.

Michigan.gov uses secure sockets layer (SSL) and/or transport layer security (TLS) technology to encrypt and protect your personal information during Internet transmissions.

**Outside links**

We provide links to other organizations through MiSACWIS. These links are provided for informational purposes only. In providing these links, we do not endorse the content, products, services, or viewpoints of these external websites. Once you leave MiSACWIS and link to an external website, MiSACWIS terms and policies no longer apply.